VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER BERICHT ÜBER DIE PATENTIERBARKEIT

(Kapitel II des Vertrags über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens)

Aktenzeichen des Anmelders oder Anwalts 2003P05083WO	**WEITERES VORGEHEN** siehe Formblatt PCT/IPEA/416	
Internationales Aktenzeichen PCT/EP2004/007378	Internationales Anmeldedatum *(Tag/Monat/Jahr)* 06.07.2004	Prioritätsdatum *(Tag/Monat/Jahr)* 07.07.2003
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK H04L9/08, G06F7/58		
Anmelder SIEMENS AKTIENGESELLSCHAFT et al.		

1. Bei diesem Bericht handelt es sich um den internationalen vorläufigen Prüfungsbericht, der von der mit der internationalen vorläufigen Prüfung beauftragten Behörde nach Artikel 35 erstellt wurde und dem Anmelder gemäß Artikel 36 übermittelt wird.
2. Dieser BERICHT umfaßt insgesamt 5 Blätter einschließlich dieses Deckblatts.
3. Außerdem liegen dem Bericht ANLAGEN bei; diese umfassen
   a. ☒ *(an den Anmelder und das Internationale Büro gesandt)* insgesamt 5 Blätter; dabei handelt es sich um
      ☒ Blätter mit der Beschreibung, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit Berichtigungen, denen die Behörde zugestimmt hat (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsvorschriften).
      ☐ Blätter, die frühere Blätter ersetzen, die aber aus den in Feld Nr. 1, Punkt 4 und im Zusatzfeld angegebenen Gründen nach Auffassung der Behörde eine Änderung enthalten, die über den Offenbarungsgehalt der internationalen Anmeldung in der ursprünglich eingereichten Fassung hinausgeht.
   b. ☐ *(nur an das Internationale Büro gesandt)*i> insgesamt (bitte Art und Anzahl der/des elektronischen Datenträger(s) angeben) , der/die ein Sequenzprotokoll und/oder die dazugehörigen Tabellen enthält/enthalten, nur in computerlesbarer Form, wie im Zusatzfeld betreffend das Sequenzprotokoll angegeben (siehe Abschnitt 802 der Verwaltungsvorschriften).

4. Dieser Bericht enthält Angaben zu folgenden Punkten:

☒	Feld Nr. I	Grundlage des Bescheids
☐	Feld Nr. II	Priorität
☐	Feld Nr. III	Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
☐	Feld Nr. IV	Mangelnde Einheitlichkeit der Erfindung
☒	Feld Nr. V	Begründete Feststellung nach Arikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
☐	Feld Nr. VI	Bestimmte angeführte Unterlagen
☐	Feld Nr. VII	Bestimmte Mängel der internationalen Anmeldung
☐	Feld Nr. VIII	Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags	Datum der Fertigstellung dieses Berichts
31.01.2005	26.09.2005
Name und Postanschrift der mit der internationalen Prüfung beauftragten Behörde Europäisches Patentamt - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Bevollmächtigter Bediensteter Liebhardt, I Tel. +31 70 340-4114

INTERNATIONALER VORLÄUFIGER BERICHT ÜBER DIE PATENTIERBARKEIT

Internationales Aktenzeichen
PCT/EP2004/007378

Feld Nr. I Grundlage des Berichts

1. Hinsichtlich der **Sprache** beruht der Bericht auf der internationalen Anmeldung in der Sprache, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

   ☐ Der Bericht beruht auf einer Übersetzung aus der Originalsprache in die folgende Sprache, bei der es sich um die Sprache der Übersetzung handelt, die für folgenden Zweck eingereicht worden ist:
   - ☐ internationale Recherche (nach Regeln 12.3 und 23.1 b))
   - ☐ Veröffentlichung der internationalen Anmeldung (nach Regel 12.4)
   - ☐ internationale vorläufige Prüfung (nach Regeln 55.2 und/oder 55.3)

2. Hinsichtlich der **Bestandteile*** der internationalen Anmeldung beruht der Bericht auf *(Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt)*:

Beschreibung, Seiten	
1-15	in der ursprünglich eingereichten Fassung
Ansprüche, Nr.	
4-11	eingegangen am 31.01.2005 mit Schreiben vom 24.01.2005
1-3, 12-23	eingegangen am 10.08.2005 mit Schreiben vom 05.08.2005
Zeichnungen, Blätter	
1/4-4/4	In der ursprünglich eingereichten Fassung

   ☐ einem Sequenzprotokoll und/oder etwaigen dazugehörigen Tabellen - siehe Zusatzfeld betreffend das Sequenzprotokoll

3. ☐ Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:
   - ☐ Beschreibung: Seite
   - ☐ Ansprüche: Nr.
   - ☐ Zeichnungen: Blatt/Abb.
   - ☐ Sequenzprotokoll *(genaue Angaben)*:
   - ☐ etwaige zum Sequenzprotokoll gehörende Tabellen *(genaue Angaben)*:

4. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der diesem Bericht beigefügten und nachstehend aufgelisteten Änderungen erstellt worden, da diese aus den im Zusatzfeld angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2 c)).
   - ☐ Beschreibung: Seite
   - ☐ Ansprüche: Nr.
   - ☐ Zeichnungen: Blatt/Abb.
   - ☐ Sequenzprotokoll *(genaue Angaben)*:
   - ☐ etwaige zum Sequenzprotokoll gehörende Tabellen *(genaue Angaben)*:

* *Wenn Punkt 4 zutrifft, können einige oder alle dieser Blätter mit der Bemerkung "ersetzt" versehen werden.*

Feld Nr. V Begründete Feststellung nach Artikel 35 (2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja:	Ansprüche	1-23
	Nein:	Ansprüche	
Erfinderische Tätigkeit (IS)	Ja:	Ansprüche	1-23
	Nein:	Ansprüche	
Gewerbliche Anwendbarkeit (IA)	Ja:	Ansprüche:	1-23
	Nein:	Ansprüche:	

2. Unterlagen und Erklärungen (Regel 70.7):

siehe Beiblatt

Zu Punkt V

Begründete Feststellung hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

Es wird auf das folgende Dokument verwiesen:
D1: WO 97/49213 A (ERICSSON GE MOBILE INC) 24. Dezember 1997 (1997-12-24)

1. Das Dokument D1 wird als nächstliegender Stand der Technik gegenüber dem Gegenstand des Anspruchs 1 angesehen. Es offenbart ein Verfahren zur Datenübertragung mit folgenden Schritten:
   - Eingabe von ersten Daten aus einem stochastischen Prozeß in zumindest erste und zweite Teilnehmer eines Kommunikationsnetzes (Seite 4, Zeile 24 bis Seite 5, Zeile 14);
   - in jedem der zumindest ersten und zweiten Teilnehmer:
     Erzeugung eines symmetrischen Schlüssels, basierend auf den ersten Daten und Speicherung des symmetrischen Schlüssels für eine verschlüsselte Datenübertragung zwischen den zumindest ersten und zweiten Teilnehmern (Seite 5, Zeilen 9, 10 und 13, 14).

1.1. Der Gegenstand des Anspruchs 1 unterscheidet sich daher von dem bekannten Verfahren dadurch, dass jeder der zumindest ersten und zweiten Teilnehmer über Mittel für zumindest ein erstes und ein zweites Verschlüsselungsverfahren zur Schlüsselerzeugung verfügt, wobei basierend auf den ersten Daten jeweils erste bzw. zweite symmetrische Schlüssel erzeugt werden, und dass für die verschlüsselte Datenübertragung in zeitlicher Reihenfolge zwischen den Verschlüsselungsverfahren gewechselt wird.

1.2. Der Gegenstand des Anspruchs 1 ist somit neu (Artikel 33(2) PCT).

1.3. Die mit der vorliegenden Erfindung zu lösende Aufgabe kann somit darin gesehen werden, dass mit einem vergleichsweise geringem Aufwand das Sicherheitsniveau

der Verschlüsselung gemäß D1 erhöht werden soll.

Die in Anspruch 1 der vorliegenden Anmeldung für diese Aufgabe vorgeschlagene Lösung beruht aus den folgenden Gründen auf einer erfinderischen Tätigkeit (Artikel 33(3) PCT):

Obgleich eine zeitlich wechselnde Verwendung verschiedener alternativer Verschlüsselungsverfahren zur Datenverschlüsselung in ein und demselben Verschlüsselungssystem prinzipiell bekannt ist, ist eine Zeitlich variierende **Schlüsselerzeugung** dem Fachmann nicht gebräuchlich. Weder aus dem Dokument D1 alleine noch aus einer Kombination von D1 mit anderen Dokumenten gehen die technischen Merkmale des kennzeichnenden Teils des Anspruchs 1 auf eine dem Fachmann offensichtliche Weise hervor.

2. Die oben genannten Begründungen gelten ebenfalls für die unabhängigen Ansprüche 14 und 17. Der Gegenstand der Ansprüche 14 und 17 ist somit ebenfalls neu (Artikel 33(2) PCT) und beruht auch auf einer erfinderischen Tätigkeit (Artikel 33(3) PCT).

3. Die Ansprüche 2-13, 15, 16 und 18-23 sind von den Ansprüchen 1, 14 oder 17 abhängig und erfüllen damit ebenfalls die Erfordernisse des PCT in bezug auf Neuheit und erfinderische Tätigkeit.

4. Bei dem Eintritt in die regionale Phase sollte darauf geachtet werden, den Stand der Technik (Dokument D1) zu würdigen und die Beschreibung an die dann gültige Fassung der Ansprüche anzupassen.

Patentansprüche

1. Verfahren zur Datenübertragung mit folgenden Schritten:

- Eingabe von ersten Daten aus einem stochastischen Prozess (114) in zumindest erste und zweite Teilnehmer (102, 104; 402, 404; 502, 504, 506, 508, 510, 512, 516) eines Kommunikationsnetzes (100, 106; 400, 406; 500, 514, 518),

- in jedem der zumindest ersten und zweiten Teilnehmer: Erzeugung eines symmetrischen Schlüssels (S1, S2), basierend auf den ersten Daten und Speicherung des symmetrischen Schlüssels für eine verschlüsselte Datenübertragung zwischen den zumindest ersten und zweiten Teilnehmern,

dadurch gekennzeichnet,

dass jeder der zumindest ersten und zweiten Teilnehmer über Mittel (108; 408) für zumindest ein erstes und ein zweites Verschlüsselungsverfahren zur Schlüsselerzeugung verfügt, wobei basierend auf den ersten Daten jeweils erste bzw. zweite symmetrische Schlüssel erzeugt werden, und dass für die verschlüsselte Datenübertragung in zeitlicher Reihenfolge zwischen den ersten und zweiten Verschlüsselungsverfahren gewechselt wird.

2. Verfahren nach Anspruch 1, wobei zur Erzeugung der ersten und zweiten Schlüssel in jedem der zumindest ersten und zweiten Teilnehmer verschiedene erste Daten durch unterschiedliche Kombinatorik der stochastischen Daten gebildet werden.

3. Verfahren nach Anspruch 1 oder 2, wobei die ersten Daten über das Kommunikationsnetz (100, 106; 400, 406; 500, 514, 518) übertragen werden.

4. Verfahren nach einem der vorhergehenden Ansprüche, wobei die ersten Daten durch Erfassung von mindestens einem Messwert aus dem stochastischen Prozess (114) gewonnen werden.

5. Verfahren nach einem der vorhergehenden Ansprüche, wobei es sich bei dem stochastischen Prozess um einen zeitlich veränderlichen Parameter eines Automatisierungssystems (500) handelt.

6. Verfahren nach einem der vorhergehenden Ansprüche, wobei die ersten Daten aus niedersignifikanten Bit-Positionen (LSB) eines oder mehrerer Messwerte gewonnen werden.

7. Verfahren nach einem der vorhergehenden Ansprüche, wobei jeder der zumindest ersten und zweiten Teilnehmer stochastische Daten erfasst, aus denen die ersten Daten gebildet werden.

8. Verfahren nach Anspruch 7, wobei die ersten Daten aus den stochastischen Daten durch eine vorgegebene Kombinatorik gebildet werden.

9. Verfahren nach Anspruch 7 oder 8, wobei die stochastischen Daten über das Kommunikationsnetz (100, 106; 400, 406; 500, 514, 518) übertragen werden.

10. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Erzeugung des symmetrischen Schlüssels in den Teilnehmern auf Anforderung eines Master-Teilnehmers des Kommunikationsnetzes erfolgt.

11. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Erzeugung des symmetrischen Schlüssels zu vorbestimmten Zeitpunkten oder nach vorbestimmten Zeitintervallen in den zumindest ersten und zweiten Teilnehmern erfolgt.

12. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Übertragung der ersten Daten oder der stochastischen Daten zu einem Zeitpunkt geringer Auslastung des Kommunikationsnetzes erfolgt.

13. Verfahren nach einem der vorhergehenden Ansprüche, wobei die Übertragung der ersten Daten oder der stochastischen Daten mit einem asymmetrischen Verschlüsselungsverfahren erfolgt.

14. Computerprogrammprodukt, insbesondere digitales Speichermedium, mit Programmmitteln zur Durchführung der folgenden Schritte:

- Eingabe von ersten Daten aus einem stochastischen Prozess (114) in zumindest erste und zweite Teilnehmer (102, 104; 402, 404; 502, 504, 506, 508, 510, 512, 516) eines Kommunikationsnetzes (100, 106; 400, 406; 500, 514, 518),

- in jedem der zumindest ersten und zweiten Teilnehmer: Erzeugung eines symmetrischen Schlüssels (S1, S2), basierend auf den ersten Daten und Speicherung des symmetrischen Schlüssels für eine verschlüsselte Datenübertragung zwischen den zumindest ersten und zweiten Teilnehmern,

dadurch gekennzeichnet,

dass jeder der zumindest ersten und zweiten Teilnehmer über Mittel (108; 408) für zumindest ein erstes und ein zweites Verschlüsselungsverfahren zur Schlüsselerzeugung verfügt, wobei basierend auf den ersten Daten jeweils erste bzw. zweite symmetrische Schlüssel erzeugt werden, und dass für die verschlüsselte Datenübertragung in zeitlicher Reihenfolge zwischen den Verschlüsselungsverfahren gewechselt wird.

15. Computerprogrammprodukt nach Anspruch 14, wobei die ersten Daten durch Erfassung eines Messwerts aus dem stochastischen Prozess (114) gewonnen werden.

16. Computerprogrammprodukt nach Anspruch 14 oder 15, wobei die ersten Daten aus niedersignifikanten Bit-Positionen (LSB) eines oder mehrerer Messwerte gewonnen werden.

17. Kommunikationssystem mit zumindest ersten und zweiten Teilnehmern (102, 104; 402, 404; 502, 504, 506, 508, 510, 512, 516) und einem Kommunikationsnetz (100, 106; 400, 406; 500, 514, 518) für eine Datenübertragung zwischen den zumindest ersten und zweiten Teilnehmern, und mit:

- Mitteln (112) zur Eingabe von ersten Daten aus einem stochastischen Prozess (114) in die zumindest ersten und zweiten Teilnehmer,

- in jedem der zumindest ersten und zweiten Teilnehmer: Mittel (108; 408) zur Erzeugung eines symmetrischen Schlüssels basierend auf den ersten Daten und Mittel (110; 426; 520, 522) zur Speicherung des symmetrischen Schlüssels für eine verschlüsselte Datenübertragung zwischen den zumindest ersten und zweiten Teilnehmern,

dadurch gekennzeichnet,

dass jeder der zumindest ersten und zweiten Teilnehmer über Mittel (108; 408) für zumindest ein erstes und ein zweites Verschlüsselungsverfahren zur Schlüsselerzeugung verfügt, wobei basierend auf den ersten Daten jeweils erste bzw. zweite symmetrische Schlüssel erzeugt werden, und dass für die verschlüsselte Datenübertragung in zeitlicher Reihenfolge zwischen den Verschlüsselungsverfahren gewechselt wird.

18. Kommunikationssystem nach Patentanspruch 17, wobei es sich bei dem Kommunikationsnetz (100, 106; 400, 406; 500, 514, 518) um ein öffentliches Netz handelt.

19. Kommunikationssystem nach Patentanspruch 17 oder 18, wobei es sich bei dem Kommunikationsnetz (100, 106; 400, 406; 500, 514, 518) um das Internet handelt und ein Teilnehmer als Master-Teilnehmer ausgebildet ist, um eine Schlüsselerzeugung in den anderen Teilnehmern durch Übertragung einer entsprechenden Anforderung über das Internet auszulösen.

20. Kommunikationssystem nach Anspruch 17 oder 18, wobei es sich bei dem Kommunikationsnetz (100, 106; 400, 406; 500, 514, 518) um ein Ethernet handelt.

21. Kommunikationssystem nach Anspruch 20, wobei einer der Teilnehmer als Master-Teilnehmer ausgebildet ist, um auf das Ethernet ein Kommando zur Auslösung der Schlüsselerzeugung in den Teilnehmern auszugeben.

22. Kommunikationssystem nach einem der vorhergehenden Ansprüche 17 bis 21, wobei es sich bei den zumindest ersten und zweiten Teilnehmern um Komponenten eines Automatisierungssystems (500) handelt.

23. Kommunikationssystem nach einem der vorhergehenden Ansprüche 17 bis 22, wobei zumindest einer der Teilnehmer (516) zur Durchführung einer Fernwartung ausgebildet ist.